

REMARKS

This amendment responds to the Office Action dated July 6, 2005. The examiner provisionally withdrew certain claims (48-62, 78-89 and 153-160) from consideration because no generic claim was allowed. As stated later, applicant respectfully requests that the examiner find that the presently amended independent claims (63, 90, 224) are patentable and reinstate claims 48-62, 78-89 and 153-160 provided applicant amends those claims in accordance with claim 63 herein.

Due to the complex nature of the Lamm '907 system, applicant requests an interview with the examiner and the SPE assigned to this case to discuss the reference and the amended claims.

The examiner issued a double patenting rejection (see Office Action pages 9-13, para. 17-24) based upon Serial Nos. 10/008,209; 10/008,218; 10/155,525; 10/155,192; 10/277,196; and 10/390,807. These applications are all owned by applicant. Applicant requests that this requirement be postponed until after an allowable claim or claims have been approved. Applicant will file terminal disclaimers if necessary. This topic can be addressed at the interview.

In the Office Action on pages 2-3, paragraphs 5-8, the patent examiner questions the use of certain language in claim 91 (a rejection under 35 U.S.C. §112). Claim 91 has been amended to correct this typographic error referring to the extract store and remainder store memories.

In the Office Action on pages 9-16, paragraphs 5-8, the patent examiner rejects all claims 63-77; 90-101; and 224-234 as being non-patentable under 35 U.S.C. §§ 102 or 103 in view of certain prior art or pre-existing technology disclosed in the following references:

U.S. Patent No.6,078,907 to Lamm

U.S. Patent No.6,598,161 to Kluttz

U.S. Patent No.5,036,315 to Gurley

The 1996 book, Applied Cryptography, by Schneier (attached to Office Action)

The Uniform Resource Locator article “FOLD OC” (attached to Office Action)

Summary

In summary, Lamm ‘907 stores the secret or secured data about the consumer in three (3) different computers, to wit, consumer computer 12, billing - processor computer 26 (see col. 13, line 5) and enrollment server 21 (see col. 9, line 42). The non-secret or non-sensitive data is transmitted via Internet 28 and is merged with secret data by all three computers (a) without the need or the “presence” of a security code prior “to obtain[ing] access to said extract store” (claim 63); and, (b) access to the secret data by all three computers is permitted without the need to present a security code clearance. Claim 63 in the present case recites “presenting a predetermine security clearance to obtain access to said extract store; and permitting reconstruction of said data and remainder data only in the presence of said predetermined security clearance after presentment thereof.” These are the major differences (“security clearance to obtain access” and reconstruction “only in the presence of said predetermined security clearance after presentment thereof”) between Lamm ‘907 and the claimed invention.

Lamm ‘907

In Lamm ‘907, consumer computer 20 (FIG. 2) includes an unsecured billing information database 37 and a secured billing information database 38. The unsecured database has bill component files 34 that are graphical image and text files which can be used to generate conventional bills. Col. 5, lines 49-58. The secured billing information database 38 in consumer computer 20 includes user profile database 40,

billers profile database 42 and payment account database 44. Col. 6, lines 3-15. For example the consumer's social security number is secured billing data. col. 6, line 10.

The consumer's computer is the first computer to store secured data.

Billing messages 18 are sent via the Internet 28 by the billing processor computer 26 (FIG. 1) in a redacted content form with only non-sensitive content. Col. 6, lines 26-28. Payment instructions 19 are also sent with only redacted, non-sensitive content. Col. 6, line 31. The billing messages 18 and payment instruction messages 19 "are anonymous messages in which the billed party's name, social security number, address, and other identifying information is not present ... [and] such identifying information would be impossible to obtain based solely on the information that the messages in the electronic post office 16 contain" col. 6, lines 32-37 (emphasis added). "The billing messages 18 are redacted so that the billed party remains anonymous." Col. 7, lines 17-19. The electronic post office (E.P.O.) (FIGS. 1 and 3) "functions primarily as a dedicated e-mail server." Col. 6, line 57. The bills 18 are redacted so that the billed party (consumer) remains anonymous to others. Col. 7, line 17. FIG. 1 shows billing processor computer 26 includes processor computer 20 and legacy computer 24.

The processor computer 20 (FIGS. 1 and 4) includes two databases, one for secured data 79 and the other for unsecured data 71 (redacted bill files 77). Col. 7, lines 60, 64. The processor computer 20 (Fig. 4) may include redacting instructions 80 to remove secured billing information from bills. Col. 8, lines 24-27.

The processor computer 20 is the second computer that stores secured data.

FIG. 5 shows three processes (see left side labels) - - registration/enrollment; presentation of bills from vendor-billing party to consumer-billed party; and payment---. During enrollment, the consumer-billed

party gives the service provider- 3rd party payor, operating the enrollment server 21, secured billing information (credit card numbers). Col. 9, lines 40-45. This secured data is stored in enrollment database 25 or authentication database 17 (FIGS. 1; 3).

The enrollment data base computer is the third computer to store secured data.

Redacting instructions 116, FIG. 5, in processor computer 20 redacts all secured billing information from the full bills (col. 10, l. 21) sent from the billing vendor party. Col. 10, lines 40-44. Full bills are stored in the legacy computer 24. Col. 13, line 5. The redacted bill files contain only non-sensitive billing information sent to the EPO or electronic post office (operated by the service provider). Col. 10, lines 45-57; see FIG. 5. The process of redacting includes any method of removing, deleting or editing the secured billing information from the full bill print file. Col. 10, lines 57-60. One method of redacting is to search for a particular field at a certain positional location on the paper bill such as name or address and redacting data from that field. Col. 10, line 64. However, knowledge of the location of pre-existing “secret” fields of data is required.

Lamm ‘907 does not disclose random or non-format driven redaction. Lamm only extracts data from predefined billing formats. Positional directions from legacy vendor computer 24 may be provided to the other internal vendor processor computer 20. Col. 11, lines 31-41. Computers 20 and 24 are part of billing processor computer 26. Col. 5, line 18. “These positional directions may then be sent with the redacted bill print files 70 to consumer computer 12.” Col. 11, lines 41-44. An encryption program may be used to encrypt the non-sensitive information in the redacted bill. Col. 11, lines 3-7. The redacting program, after identifying the secured-secret information from a particular known field, may remove all further instances of the same information anywhere it appears in the remainder of the full bill print file. Col.

10, lines 66- Col. 11 line 1. Graphic information or elements from the bill can be removed. Col. 11, line 9. Lamm '907 does not show random extraction nor white list or black list extraction. At best, Lamm '907 only shows positional extraction of secret data from pre-defined bill formats.

The graphic information is also stored in the consumer computer 12. Col. 11, lines 13-16. The bill print file 70 received from the billing-vendor party contains positional directions to show where the non-secured text fits into the graphic overlays representing a full or complete bill for the consumer computer. Col. 11, line 31. A record of positional directions for the bill print file 70 may be kept after the secured-secret information is striped from the full billing print file or information. Col. 11, lines 38-41. The positional directions may be sent with the redacted bill to the consumer computer 12. Col. 11, line 42. These positional directions may be used to determine where to insert the secured information to reconstruct the bill on consumer computer 12. Col. 11, lines 41-47. Only one positional relationship of the elements must be recognized. Col. 11, line 52.

In one embodiment, the non-sensitive billing information is transmitted to the consumer's computer. Col. 11, line 65. The consumer's computer reconstructs the bill for review of the reconstructed bill. Col. 12, line 10. Since the consumer's computer stores the secured data, there is no need to present a security clearance code. Since the data transmission contains no security data, the consumer does not use a password. Upon request of the consumer and at the consumer's computer, the non-sensitive billing information from billing history database 36 (part of consumer computer 12, FIG. 1) is integrated with the standard bill component files 34 (part of consumer computer 12, FIG. 1) and the secured billing information databases 38 which are also part of consumer computer 12. FIG. 1. The reconstructed bill contains all the information and graphic or standard text elements that a customer or paper bill contains. Col. 12, lines

18-30. "This information from the secured billing information database 38 can appear on the reconstructed bill 154 even though it was not sent with the non-sensitive billing information to the consumer's computer 12, because it is stored locally on the consumer's computer 12. An encryption program 36 may be used on the consumer's computer 12 if data sent from the processing computer system 20 is encrypted." Col. 12, lines 36-43 (emphasis added).

The secured billing information in customer profile database 83 [FIG. 4, part of processor computer 20] should be sufficient to allow the billing party or processor to charge a consumer's credit account or withdraw money from a consumer's bank account upon authorization from the consumer. As noted earlier, an authentication identifier, such as an EPO-mail address supplemented by a password, is set up to allow the processor or billing party to receive payment instructions from a consumer without the transfer of secured billing information. The consumer could also set up separate codes corresponding to different payment methods, such as withdrawal from the consumer's bank account or a credit charge to the consumer's credit account. These codes, also called funds source identifiers, would allow the processor to identify a funds source associated with a payment option. At block 110, the consumer receives payment information from the billing party. At block 112, the processor logs the enrollment of the consumer in the electronic payment system 10 for the billing party's records. The consumer must, in one embodiment, enroll separately or together with each billing party from which the consumer desires to obtain electronic bills.

Lamm '907, col. 9, line 57 - col. 10, line 11.

The service provider (E.P.O. Server 16, FIG. 5) is part of the third computer system which stores secured data.

Lamm '907 Comparison

In contrast to Lamm '907, the present invention reconstructs (i) after the confirmed input of a security code and (ii) only in the presence of security clearance and (iii) only obtains data from an extract store having the security sensitive words, etc. after presentment of a security code. No security code clearance is necessary in Lamm '907 to access the secured data extract store because in Lamm '904, three

(3) computers store the secured data. The present invention does not permit access to the secured information in the extract store until after presentment of the security code and does not permit reconstruction until after presentment of the security code.

The secured billing information and non-secured standard bill components are stored locally on the consumer's computer in Lamm '907. Col. 12, line 54. The non-sensitive billing information in the redacted bill file 150 may consist of an amount due, dates of the billing, due date for the bill, other bill details and a randomly assigned the bill identification number. Col. 13, lines 22-26. Redacted or non-secure data bill file 150 is stored locally on the consumer's computer 12. Col. 13, line 42. Throughout Lamm's process, only non-sensitive information is sent on the Internet. Col. 13, line 48.

In Lamm, the standard bill component files 34 (secret data) are only transmitted from billing processor computer 20 to the electronic post-office E.P.O. 16 the first time a new billing format is to be delivered to the consumer. Col. 14, lines 18-21. Alternatively, if the standard bill components (secret data) are not previously stored on the consumer's computer, the program on the consumer's computer 12 may request delivery of the standard bill components from electronic post-office 16. Col. 14, line 48. Once the standard bill components file is stored on the consumer's computer, it is not necessary to resend those component files to the consumer's computer again. Col. 14, line 60.

Therefore, Lamm '907 distributes the secret data to many computers in the system without requiring, prior to each access of the store of secret data, a security code clearance. The secret data is stored in consumer computer 12, in enrollment computer 21 (col 9, l. 42) and in processor computer 20, 24 (col. 13, l. 5). No security code clearance is needed at any of these computers to access or to reconstruct because the secret data is stored locally in all three (3) computers.

Regarding payment of the bills, payment instructions 152 (Fig. 5) from consumer at block 122 contains only non-sensitive information such as data to pay the bill, amount to pay and a funds source identifier. Col. 15, lines 50-54. The “funds source” is coded data. The payment instructions do not contain secured billing information. Col. 15, line 55. Further, the payment instructions may be encrypted. Col. 15, line 61. Payment instructions 152 do not contain secured billing information 76. Col. 16, line 28.

The largest difference between Lamm ‘907 and the presently claimed invention is that the secret information in the Lamm ‘907 system is widely distributed. Consumer computer 12, enrollment server 21 and billing processor computer 26 (which includes processor computer 20 and legacy computer 24) all contain secured or secret confidential information of consumer. FIG. 2 shows consumer computer 20 having secured billing information database 38. The enrollment server 21 is part of the service provider (FIG. 5) and includes an enrollment database 25 which has secured information therein. Col. 9, line 42. Of course, vendor or billing party computers 20, 24 which are part of billing processor computer 26 (FIG. 1) also include secured or secret data. Col. 7, lines 57-66. It is only the billing messages 18 sent over the Internet that do not contain secret or secured data. Col. 13, lines 29-33. “A primary consequence of this distinction is that billing messages 18 are prepared and sent by the processor server computer system 26 to the electronic post office 16 with redacted content only. Similarly, payment instruction messages 19 are prepared by consumer computer 12 and sent to the electronic post office 16 with redacted content only.” Col. 6, lines 25-32. Since the Lamm ‘907 reference includes secret data spread widely throughout the system (other than the electronic post office E.P.O. server 16 when it receives billing messages 18 (FIG. 1)), the Lamm ‘907 system could never provide a data security system as claimed in the present invention.

Applicant has amended independent claim 63 to include the step of “presenting a predetermined security clearance to obtain access to said extract store” and has clarified the “permitting reconstruction” step to provide that reconstruction is permitted “only in the presence of said predetermined security clearance after presentment thereof.” In Lamm ‘907, access to the secret data is always available to the operators of consumer computer 12, to operators of enrollment server 21 (and, by default, the service provider, see FIG. 5) and to operators of vendor-billing computers 20, 24, 26.

Support for this concept (access needs security clearance) can be found throughout the patent specification and is specifically found in FIG. 1B at clearance 126 and step 305 in FIG. 5 which requires input and approval of a security element. If the security clearance is not cleared, the system takes the NO branch from decision step 306 and after a second log-in attempt 309, the user or inquiring party is prohibited from further access to the extracted data or extract store.

With respect to Lamm ‘907, since consumer computer 12 includes secured data billing information 38 (FIG. 2), this “secret” data is provided to the service provider handling electronic post office EPO server 16 and the EPO server has access to the consumer registration database 104 (FIG. 5), as provided in enrollment step 106 and enrollment server 21 (FIG. 5). The enrollment server 21 (FIG. 4) has secret information regarding the consumer. Col. 9, line 42. The vendor or billing party system 26 includes full billing information which includes “secret” data regarding the consumer or billed party in legacy computer 24. Col. 13, line 5. Therefore, the processor computer 20, which is internally linked to legacy computer 24, also has access to that secured or secret information. In Lamm ‘907, it is only the billing messages 18 that do not carry secret information. Col. 6, lines 26-30 and col. 13, lines 29-33. Therefore, the vendor or billing party does not need to provide a security clearance code “to obtain access to said extract store.”

Also, the consumer at consumer computer 12 is not required to provide a security clearance code “to obtain access to said extract store.” Further, as originally submitted in the original claim 63, reconstruction in the present invention only occurs in the presence of predetermined security clearance. The claims specifically now recite “permitting reconstruction of said data via said extract store and remainder store only in the presence of said predetermined security clearance after presentment thereof.”

Lamm ‘907 does not show, teach or suggest “presenting a predetermined security clearance **to obtain access to said extract store**” and further does not show, teach or suggest “permitting reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment thereof.” (Claim 63, emphasis added). In the present invention, the presentment of a security code is critical (a) to obtain any access to the secured data and (b) prior to permitting reconstruction of the data and “only in the presence of said predetermined security clearance.”

Also, the Lamm ‘907 system, with its storage of secured data at three (3) locations, does not show, teach or suggest “storing said extracted data and said remainder data in said extract store and said remainder store, respectively.” Claim 63. The storage in Lamm ‘907 of secured data at three (3) locations is not the same as storing secured data “in said extract store” per claim 63.

Therefore, the presently claimed invention is different and patentably distinct from Lamm ‘907. Independent claims 90 and 224 each have substantially similar recitations compared with claim 63.

With respect to the Schneier book extract (Applied Cryptography), Schneier does not show, teach or suggest “presenting a predetermined security clearance to obtain access to said extract store; and, permitting reconstruction of said data via said extracted data and remainder data only in the presence of

said predetermined security clearance after presentment thereof.” Schneier discusses encryption and key destruction.

Kluttz ‘161 does not show, teach or suggest presenting a predetermined security clearance to obtain access to the extract store and permitting reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment thereof as required by the present invention. Kluttz ‘161 shows utilizing multiple encryption portions in a singular document. See Abstract and FIG. 3. The keys are maintained in the document 100. Col. 6, lines 28-30. FIGS. 5 and 6 show the flowcharts for document decryption which includes utilizing the encryption key in the document itself (step 304, FIG. 5; step 404, FIG. 6). There is no suggestion of utilizing an extracted store and a remainder store.

U.S. Patent No. 5,036,315 to Gurley does not cure the defects identified above with respect to Lamm ‘907 and the differences with respect to the present invention. Gurley does not show, teach or suggest (a) filtering data; (b) utilizing an extract store and a remainder store; (c) presenting a predetermined security clearance to obtain access to said extract store; and (d) permitting reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment thereof.

Lastly, the definition of Uniform Resource Locator or URL attached to the Office Action dated July 7, 2005 does not show, teach or suggest using an extract data store and a remainder data store and permitting reconstruction only in certain circumstances.

Dependent claim 68 has been amended to provide that the step of presenting “includes a plurality of presenting steps” and that the step of permitting reconstruction occurs after presentment of respective

ones of said plurality of security clearance levels. No new matter is added to this case by this change to claim 68 since support for this concept is found throughout the patent specification and particularly in FIG.

3.

Claim 68

It should be noted that Lamm '907, Schneier, Kluttz '161 nor Gurley '315 show (a) multiple security levels per claim 68, nor (b) multiple presentment levels per claim 68, nor partial reconstruction per claim 68. In fact, no reference mentions partial reconstructions.

Claim 90

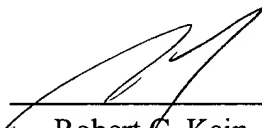
Independent claim 90 has been amended to add “presenting a predetermined security clearance to obtain access to said extract store” and to provide that reconstruction is permitted “only in the presence of said predetermined security clearance after presentment thereof.” Accordingly, claim 90 is patentably distinct over the references cited by the patent examiner.

Claim 224

Claim 224 has been amended to provide “a security clearance control, coupled to said memory store of said first and second designated computers, controlling access to said memory store of said first designated computer only in the presence of a predetermined security clearance.” Since the security clearance control only provides access to the secured data (extracted data) “in the presence of a predetermined security clearance”, the compiler can only compile and reconstruct the data from the extracted data and remainder data “dependent upon access provided by said security clearance control.” Therefore, claim 224 is patentably distinct from the references cited by the examiner.

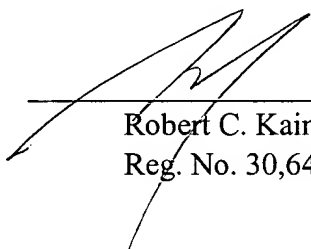
Applicant respectfully requests that the examiner approve the patentability of claims 63-77; 90-101 and 224-234. Applicant respectfully requests that the examiner permit applicant to amend the other independent claims in elected invention Group II, that is, independent claims 48, 78 and 53. With the addition of "presenting a predetermined security clearance to obtain access to said extract store," most of these claims 48, 78 and 153 (and dependent claims) become generic and patentable.

Respectfully submitted,

By 
Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco,
P.L.
750 Southeast Third Avenue, Suite 100
Fort Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 14, 2005.


Robert C. Kain, Jr.
Reg. No. 30,648

\\TIGER\Data Share\RCK\CLIENTS\Redlich\Patents\6851-02-amdt-072505.wpd